REMARKS

The present Amendment cancels claims 1-22 and adds new claims 23-44. Therefore, the present application has pending claims 23-44.

The Examiner indicated that the references in the specification were not in a proper Information Disclosure Statement to satisfy the requirement of 37 CFR §1.98(b). Attached herewith is a PTO-1449 providing a listing of said references. An indication that the Information Disclosure Statement has been considered is respectfully requested.

Claims 1, 2, 6 and 18 stand objected to due to informalities noted by the Examiner. As indicated above, claims 1, 2, 6 and 18 were canceled. Therefore, this objection is rendered moot.

Claims 14 and 18 stand rejected under 35 USC §112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regards as their invention. As indicated above, claims 14 and 18 were canceled. Therefore, this rejection is rendered moot. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

Claims 1-22 stand rejected under 35 USC §103(a) as being unpatentable over Cramer (U.S. Patent No. 6,697,488). As indicated above, claims 1-22 were canceled. Therefore, this rejection is rendered moot. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

The features of the present invention as recited in new claims 23-44 are not anticipated nor rendered obvious by Cramer. Cramer is directed to a scheme with improve the security of encrypted data or information by using a practical public

cryptosystem that is able to resist adaptive attacks. According to Cramer, the scheme does not leak any information of the secret of the used key by generating an extended private key and public key. As per Cramer, a message m, also referred to as plaintext, can be encrypted to obtain a cipher text t by using the public key. This cipher text t can be transmitted over an insecure channel such as the internet so that only a recipient with the right private key is able to decrypt the cipher text t.

The proof of security according to the system taught by Cramer is based on standard assumptions which are the hardness of the Diffie-Hellman decision problem (DDH problem), wherein the DDH problem is very hard to solve due to the large calculation volume; and the collision intractability of the hash function, which is equivalent to the existence of universal one-way functions.

Cramer employs a hash function in the encryption algorithm as described in col. 7, line 50 to col. 8, line 21 and col. 11, line 60 to col. 12, line 34 thereof. Cramer also discloses a particular encryption method using a hash function and the hash value in claims 11 and 12 thereof.

The proof of security of the present invention as described, for example, on page 4, line 26 through page 7, line 4 of the present application relates to a security system which is also based on an assumption of the hardness of the Diffie-Hellman decision problem. However, the proof security of the present invention is not based on the above described assumption regarding the collision intractability of the hash function through which the existence of the universal one-way functions are provided. In the present invention, a hash function and a hash value are not used in the encryption process.

As is well known, various cryptographic schemes are based on various assumptions. However, such assumptions are not always realistic. The collision intractability of the hash function has not yet been verified. See page 3, line 27 to page 4, line 24 of the present application. Therefore, contrary to Cramer, the present invention does not rely on the unverified assumption of the collision intractability of the hash function for encryption and as such is directed to an encryption process entirely different from Cramer.

Thus, as is quite clear from the above, the present invention is quite different from Cramer, particularly with regard to the assumptions upon. According to the present invention, hash functions and values are not used in the encryption process thereof. Therefore, the features of the present invention as recited in the claims are not taught or suggested by Cramer whether taken individually or in combination with any of the other references of record.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references utilized in the rejection of claims 1-22.

In view of the foregoing amendments and remarks, applicants submit that claims 23-44 are in condition for allowance. Accordingly, early allowance of claims 23-44 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (500.41092X00).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge

Registration No. 29,621

CIB/jdc (703) 684-1120 FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use several sheets if necessary)

ATTY. DOCKET NO.

500.41092X00

SERIAL NO. 10/046,224

APPLICANT

M. NISHIOKA, et al

FILING DATE

January 16, 2002

GROUP **2136**

(0	26 26ACH	ai silecto .					Janu	ary 16, 2002		213			
				U.S.	PAT	ENT	DOCL	JMENTS					
							_		CL	ASS	SUBCLASS	FILING DAT IF APPROPRI	E ATE
MINER AL	DOCUMEN.	T NUMBER	1 - 1				DATE	NAME				_	
			11							$-\dagger$			
										+			
				}									
						_ {							
			11							20	//	ļ	
			+-+					000	リル	ツト	·		
			+-+					15th	グサ		-		
								 	-+				
					}				+			1	
								<u> </u>				+	
						Ì							
	├		+										
OREIGN F	ATE	NT DO	CUME	NTS			1	COUNTRY		CLASS	SUBCLASS	ABSTRACT	<u> </u>
	DOCUM	IENT NUMBE	R				DATE	COUNTRY				YES	NO
	 -			1	Γ								
	 			┼	}	├	 	+			1		
					 	}	 	+			1		
				1	\	1	 			 		-	1
				1	l								+
	+-					1	}				-		+
				\top	1					<u> </u>			
		<u> </u>				 •	 T:41a [Note Pertine	nt Pac	aes. E	tc.)		
OTHER D	OCUN	IENTS	(Inclu	ding	Aut	nor,	i itie, L	ate, Pertine		d nubl	ic-key crys	otosystem	ıs,
					46-04	foro	htainino	diditai Signatu	ires an	u pubi			
	Co	mmun.	of the A	CM, V	/01. Z	1, 140.	2. pp. !	20-126, 1978.	of Cr	vpto '8	5, LNCS21	18, Spring	er-
	V. :	S. Mille	, Use (of ellip	otic ci 85.	urves	ın Cryp	tography, Proc			•		
	Ve	rlag, pp	. 411-42	.0, 100		4001	etame N	Math. Comp. 48	, 177, p	р. <u>20</u> 3	-209, 1987	·	
	N.	Koblitz	Elliptic	Curv	e Cry	/LUSY	201113, 1	EDED	<u> </u>				
EXAMINER					1		CONSID					nd not	
FXAMINER	R: Initia	al if cita	tion is (consid	lered	, drav	v line th	rough citation i	if not it dicant.	n cont	Ulliance a		
considered	d. Inclu	ude cop	y of thi	s form	n with	next	commu	nication to app (Form PTO	1449	6-41)			

FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use several sheets if necessary)

ATTY.	DOCKET	NC
VIII.	000.11	

500.41092X00

SERIAL NO. 10/046,224

APPLICANT

M. NISHIOKA, et al

FILING DATE
January 16, 2002

GROUP 2136

						0.0		1	T DOCL				FILING DATE	F	
INER								1	DATE	NAME	CLASS	SUBCLASS	IF APPROPRIA	ATE	
L		OCUME	NT NUME	BER							}				
		_	_	}							_				
1		Ì		ļ											
	_														
			-+	+							ļ				
			ļ	1							ATT.	//			
	$\neg \uparrow$								Ì		100 Z				
		-+	\dashv								<i>)\\\\\\</i>	4			
ļ	1	Ì	1									+	 		
												<u> </u>	<u> </u>		
								1	T						
		\							┼						
			l			l	<u> </u>								
OREIG	N P	ATE	NT D	OC	JME	NTS									
			MENT N						DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT YES N		
													YES		
								-						-	
				 	 	 	 				1	_		L	
				├	├ ─	├	+-								
	}						1						+		
							1	ł						├-	
	+	┼─	┼	+	1	1	1							L	
	-	<u> </u>	}	+-		┼	+	+							
	1				<u> </u>										
	- DC	CIL	VEVI.	TS /I	nchi	dina	ι A u	thor.	Title, D	ate, Pertinen	t Pages,	Etc.)			
JIHE	Y DC		ILLIA	. 5 (,,,,,,,	<u> </u>	· · · · ·		a Dublic	key Encryption	s as Intrac	table as Fac	torization,	, M	
		I To	chnic	al Re	port.	IVII I / L	LUSI	LWIA	3141100101						
	1	1					_		-4	ad a Signature	Scheme Ba	sed on Disc	rete		
	-	Lo	garith	hms.	IEEE,	1 ran	15. O	1 IIIIO	illiauoii i	110019, 11_0 1, 17	<u> </u>			_	
	\top	9	Gold	wass	er. et	al Pr	obal	oilistic	Encrypti	on, JCSS, 28, 2	, pp. 270-2	99, 1984.			
EXAMI	LL NER	1 0.	<u> </u>		, 				CONSIDE						
							- 1					formance ar	-		

SHEET 3 OF 5 SERIAL NO. ATTY, DOCKET NO. FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office 10/046,224 500.41092X00 INFORMATION DISCLOSURE APPLICANT STATEMENT BY APPLICANT M. NISHIOKA, et al **GROUP** FILING DATE (Use several sheets if necessary) 2136 January 16, 2002 U.S. PATENT DOCUMENTS FILING DATE
IF APPROPRIATE SUBCLASS NAME CLASS DATE EXAMINER INITIAL DOCUMENT NUMBER FOREIGN PATENT DOCUMENTS ABSTRACT SUBCLASS CLASS COUNTRY DATE DOCUMENT NUMBER YES OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.) M. Blum et al, An Efficient Probabilistic Public-key Encryption Scheme which hides all Partial Information, Proc. of Crypto '84, LNCS196, Springer-Verlag, pp. 289-299, 1985. S. Goldwasser, et al, Lecture Notes on Cryptography, http://www-cse, ucsd.edu/users/mihir/1997. T. Okamoto, et al, A new Public-key Cryptosystem as Secure as Factoring, Proc. of Eurocrypt '98, LNCS1403, Springer Veriag, pp. 308-318, 1998.

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EXAMINER

DATE CONSIDERED

SHEET 4 OF 5

NOV 1 7 2005 SERIAL TRABE

FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use several sheets if necessary)

ATTY. DOCKET NO.

500.41092X00

10/046,224

APPLICANT

M. NISHIOKA, et al

FILING DATE
January 16, 2002

GROUP **2136**

(Use several sheets if necessary)								Janu	January 16, 2002 2136						
						u.s	. PA	TEN	T DOC	JMENT	S	 -			
WINES									DATE		AME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE	
MINER IAL		DOCUMENT NUMBER													
	_		-+	}		-+									
\						_							. 11		
		1								 		1	M		
										ļ	-51	Alla	2 11 -		
										<u> </u>		W IN IN		 	
	-+	+	+	+											
								 							
							<u> </u>	J							
OREIG	iN P	ATE	NT C	ocl	JME	NTS							SUBCLASS	ABSTRACT	
ONLE			MENT NL						DATE		COUNTRY	CLASS	SOBCLASS	YES	NO
					,			π	 				 		
			}			L	<u> </u>		 				 		
	1						١ _	1					 		
	+	 	 						ļ	<u> </u>			 	_	
	┼				┼	 	+-	1							
	1_			┼	┼	┼─	+-	+	1	_					<u> </u>
		<u> </u>	<u> </u>		 	-		+-							\
		1	\ _		<u> </u>					l			<u>-l</u>		
OTUE	D D(CUI	MEN.	TS (I	nclu	ding	ι Au	thor,	Title, D	ate, Pe	rtinent F	Pages, E	tc.)		
UIRE		T -			l Non	_Mal	leabl	e Crv	otograph	ıy, In 23 rd	Annual A	CM Sym	posium on	Theory of	
		D.	Dolve mpu	e, et a ting, p	pp. 54	2- <u>55</u>	2, 19	91.						A A 440	oke
	+-	T .			. D. bi	ia ka	w Cr	vntos	ystems F	rovably	Secure A	gainst Ch	osen Ciph	ertext Alla	icks,
		Pr	OC. 0	f STO	C, AC	M P	ress,	pp. 4	27-437, 1	990			L DEA De	oc of Furd	crvp
					A =1 66	\ntin	nal A	evmn	netric En p. 92-11	cryption	How to Er	ncrypt wi	th RSA, Pr		
EXAM	NER							DATE	CONSID	ERED					
FXAM		: Initi	ial if o	itatio	n is c	onsi	idere	d, dra	w line th	rough cit	tation if no	ot in conf ant.	ormance a	nd not	

NOV 1 7 2005 SHEET 5 OF 5 SERIAL NO. ATTY. DOCKET NO. FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office 10/046,224 500.41092X00 INFORMATION DISCLOSURE APPLICANT STATEMENT BY APPLICANT M. NISHIOKA, et al GROUP (Use several sheets if necessary) FILING DATE 2136 January 16, 2002

							T	T DOCU				FILING DA	
INER		00.045517.5	MDED					DATE	NAME	CLASS	SUBCLASS	IF APPROPR	NATE
TIAL T	— ^D	OCUMENT N	T										
	-		↓		\rightarrow								
ļ		1	1 1		1								
	_	_	11							1			
		$-\!\!\!\!+\!\!\!\!\!-$	+										
1	-	1	}								- 11		
											\mathcal{M}		
				\vdash	+				6		11	}	
1		\ \ \						 			1 0	ļ ———	
			ŀ		1]		2		 	
	-+		+										
		_		 			 	 +		_			
		ŀ	1					<u> </u>				<u> </u>	
DREIG	N P	TENT	DOC	UME	NIS			T			SUBCLASS	ABSTRACT	
		DOCUMENT	NUMBER				DAT	DATE	DATE COUNTRY	CLASS	00000	YES	NC
	1							 			 	1 129	
				1	1		1				<u> </u>		
	-+			+		1						Ì	\
					 	 	-						
			- 1			1	\ _						┼
	┼─┼		_							Ì			<u> </u>
	11			+	+-	┼	+-	 					ł
	1 1					<u> </u>					 		+
	1				T	Ì		İ			<u> </u>		
						Т					to \		
THER	DO	CUME	NTS (I	nclu	ding	Aut	hor,	Title, Dat	te, Pertinent F	-ages, E	ιυ. <i>)</i>		
	T								Draval	hly Sacure	A Adainst A	daptive	^
, , , , _ , ,		Chase	ın Cinh	ertex	t Atta	ck. P	roc. c	or Grypto_s	8, LINCS 1402, C	<u> </u>	<u> </u>		<u> 8.</u>
711,1121	+-+	Chose	л отр.					Nations of	Security for Pu	blic-kev E	ncryption	Schemes,	, Pro
		M. Be	lare, e	t al Re	latio	ns Ar	nong	r Verlag, n	p. 26-45, 1998.				
		of Cry	pto '98	, LNC	3 140	<u> </u>	inge	. + 0.14g, p	· · · · · · · · · · · · · · · · · · ·				
		l .											
	-	_				1 -	ATE (CONSIDER	FD				
		<u> </u>				10	AIE	201101DE:					
EXAMIN						_			igh citation if no				